| Pharma

Industrial Control Systems in der Arzneimittelherstellung vor Malware schützen

OT Security

SIND IHRE INDUSTRIAL CONTROL SYSTEMS SICHER VOR CYBERABGRIFFEN?

In der Arzneimittelherstellung sind Sie daran gewöhnt, hohe Sicherheitsanforderungen einzuhalten. Denn schon die kleinste Abweichung von einer Rezeptur oder ein minimaler Fehler im Prozess kann zwischen Leben und Tod entscheiden. Als Security-Verantwortlicher beschäftigen Sie sich daher mit vielen Regularien.

Die Good Manufacturing Practice (GMP) schreibt zum Beispiel die Absicherung und Überprüfbarkeit der Prozesse vor und fordern unter anderem Maßnahmen zum Schutz der Datenintegrität. Vielleicht zählt Ihr Unternehmen auch zu den Pharmaherstellern, die unter die KRITIS-Verordnung fallen und dem IT-Sicherheitsgesetz unterliegen.

Was Ihnen dabei vor allem Kopfzerbrechen bereitet, sind die Industrial Control Systems (ICS). Denn sie haben oft einen veralteten, ungepatchten Betriebssystemstand und sind dadurch besonders verwundbar. Angriffe müssen gar nicht direkt aus dem Internet kommen. Auch der Wartungstechniker, der sein Notebook anschließt, kann Malware einschleppen.

DAS DILEMMA ZWISCHEN ANFORDERUNGEN UND MACHBARKEIT

Wie schaffen Sie es, einen Security-Prozess zu etablieren, um Ihre ICS zu schützen? Herkömmliche Methoden greifen hier nicht, denn:

Auf einigen Industriesteuerungen dürfen Sie keine Security-Software installieren, da sonst die Herstellergarantie erlischt.

Sie können nicht riskieren, dass die Security-Maßnahmen in irgendeiner Weise die Performance oder Verfügbarkeit der Systeme beeinträchtigen.

Sie haben keine Möglichkeit zu prüfen, ob der Laptop des Service-Technikers mit Malware infiziert ist, können ihm aber auch nicht den Zugriff auf die Produktionssysteme verwehren.

BEST PRACTICES FÜR ICS-SECURITY

Mit einem spezialisierten Security-Tool können Sie Ihre Produktionsumgebung vor Malware schützen, ohne Software zu installieren und in die Systeme einzugreifen. Der Stick wird einfach per USB angesteckt und scannt das ICS oder das Notebook des Service-Technikers auf Malware. LED-Signale zeigen den Status an. Vorab konfigurieren Sie das Tool über Ihr Arbeitsnotebook und laden die aktuellen Viren-Pattern herunter. Nach abgeschlossenem Scan stecken Sie es wieder an Ihren Rechner an und lesen Ergebnis-Protokolle aus. Mithilfe des Sticks können Sie Security-Best-Practices für ICS umsetzen:

- Vor und nach einem Wartungstermin scannen Sie die Systeme und dokumentieren, dass sie sauber und sicher sind.
- Der Wartungstechniker und alle anderen Personen, die in die Produktionsumgebung kommen, scannen ihre Geräte mit dem kleinen Tool.
- Entdeckt der Stick etwas Verdächtiges, leuchtet er rot. Er kann die Malware entweder direkt beseitigen oder erst einmal nur ein Logfile erstellen. So können Sie bei kritischen Assets Rücksprache mit dem Hersteller halten, was am besten zu tun ist.
- Sie nutzen den Stick nicht nur für Malware-Scans, sondern auch um Systeminformationen und den Patchzustand auszulesen und zentral zu dokumentieren.

TIPP

Für Systeme, auf denen Sie Software installieren dürfen, empfiehlt sich eine Application-Lockdown-Lösung. Sie stellt mithilfe einer Whitelist sicher, dass nur autorisierte Anwendungen auf dem System ausgeführt werden. Eine solche Software braucht minimale Ressourcen und beeinträchtigt den Betrieb nicht. Lesen Sie mehr über den Endpunktschutz in unserem Whitepaper.

SO ERHÖHT DER PORTABLE STICK DIE SICHERHEIT

- Ihre ICS sind vor Malware geschützt, ohne dass Sie Security-Software auf ihnen installieren müssen.
- Auch der Wartungstechniker kann seine Geräte prüfen, ohne Software zu installieren.
- Sie stellen sicher, dass niemand Malware einschleppt.
- Mit einem Stick können Sie verschiedene Betriebssysteme scannen.
- Sie gewinnen Transparenz über den Status und Schwachstellen in der gesamten Produktionsumgebung. Alle Daten lassen sich zentral speichern und auswerten.
- Sie etablieren einen Security Prozess mit dokumentierten Ergebnissen und erfüllen Sicherheitsvorschriften.

DER PARTNER AN IHRER SEITE

Mit Trend Micro TXOne erhalten Sie eine einfach anzuwendende Lösung, um Systeme in abgeschotteten Netzwerken abzusichern. TXOne ist ein Joint Venture von Trend Micro und Moxa und verbindet führende IT-Security und OT-Security mit industrietauglicher Hardware.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss."

TREND MICRO™
Securing Your Connected World